U.S. DEPARTMENT OF HOMELAND SECURITY

Office of the Press Secretary

FOR IMMEDIATE RELEASE August 14, 2003

HOMELAND SECURITY PROVIDES ADVICE ON COMBATING THE "BLASTER" INTERNET WORM

The National Cyber Security Division of the US Department of Homeland Security today issued an advisory concerning the Internet worm known as "MSBlast", "LovSan" or "Blaster" that has been infecting computers worldwide since late Monday afternoon. This worm was launched by an unknown person and infects many computers running popular Microsoft Windows operating systems, including Windows 2000 and Windows XP. The worm does not target systems running Windows 98 or Windows ME. This is a follow up to advisories published on July 24, July 30, and August 12.

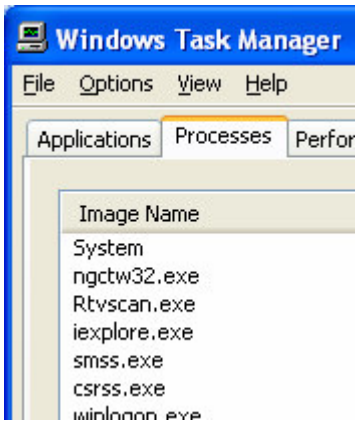
Computer users can avoid being infected by the worm by downloading a software update from Microsoft. Details on downloading and installing the update are on Microsoft's home page (www.microsoft.com).

Computer users who are already infected by the worm will receive a pop-up error message stating that the computer will reboot in 60 seconds. The computer then reboots after the timer expires, and will continue this cycle of rebooting after waiting 60 seconds.

Infected computer users should follow these steps to stop the worm and to repair the computer:

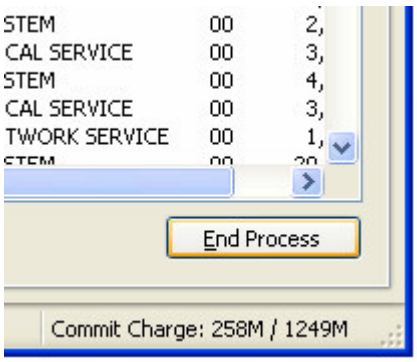
1. Physically disconnect the computer from the Internet or local network

2. Use CTRL-SHIFT-ESC to activate the Windows Task Manager

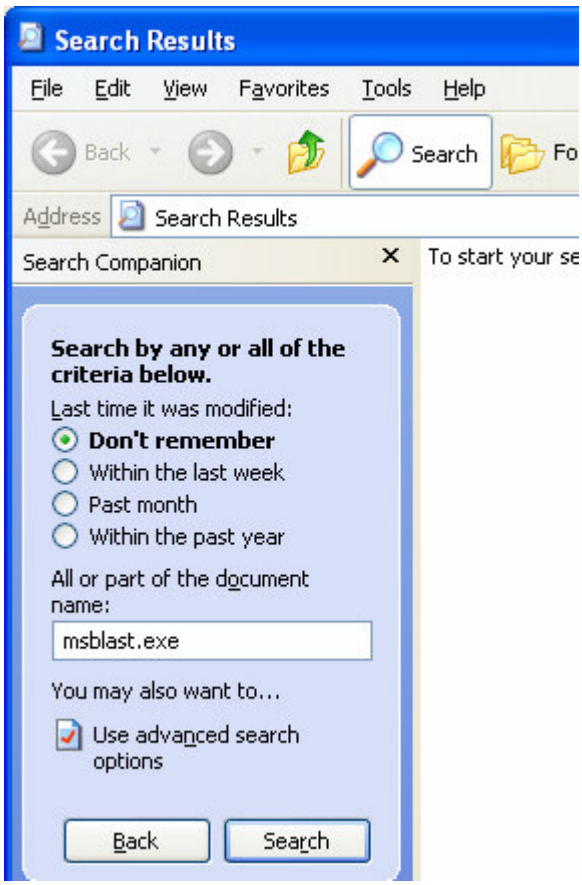


3. Click on the "Processes" tab and click on the file called "msblast.exe" (a newer version of the worm uses two new file names – "teekids.exe" or "penis32.exe", so look for either of these files if "msblast.exe" is not present)

4. Click the "End Process" button, and then close the Windows Task Manager



5. Using the file search function, search for all files called "msblast.exe", "teekids.exe" and "penis32.exe". Delete all files found with those names.



Even though the previously infected computer no longer has the worm, it is still vulnerable to a new infection if it is connected to the Internet without taking further steps to fix the software bug.

There are two ways to update the Windows operating system without getting infected again. The first method is to use another (uninfected) computer to download the upgrade

from Microsoft to a floppy disk or CD, and then copy it to the first computer. The second method is to install a firewall between the computer and the Internet before reconnecting the computer to the Internet. Specific instructions on installing a firewall and downloading updates to fix this security issue are available on Microsoft's web site at http://www.microsoft.com/security/incident/blast.asp.

Systems that remain infected after August 15th may begin flooding a Microsoft web site with thousands of requests per minute, leading to a situation known as a Denial of Service (DoS) attack. These requests will target Microsoft's update site, www.windowsupdate.com, and could lead to slowness in response or inability to reach the site for all Internet users, not just those infected by the worm.

###